Prepared Witness Testimony
Senate Committee on Commerce, Science, and Transportation
Ernest F. Hollings, Chairman

Hearing on Internet Privacy
July 11, 2001
9:30 A.M.
Senate Russell Building 253

Paul M. Schwartz
Professor of Law
Brooklyn Law School
250 Joralemon Street
Brooklyn, N.Y. 11201
<www.paulschwartz.net>

Mr. Chairman and Members of the Committee:

My name is Paul Schwartz, and I am a Professor of Law at Brooklyn Law School in Brooklyn, New York. For over a decade, I have been writing and teaching about privacy law and other areas of information law. My publications about privacy law include two co-authored reports carried out at the request of the Commission of the European Union. I have also taught courses in areas such as privacy law, Internet law, telecommunications law, and the "Law of Electronic Democracy."

Millions of Americans now engage in daily activities on the Internet, and under current technical configurations, their behavior — our behavior -- creates detailed stores of personal data. The Internet is an interactive telecommunications system, which means that computers attached to it do not merely receive information but also transmit it. Social, political and commercial life on the Internet create a finely grained data map of our interests, our beliefs, and our interpersonal relationships. This personal information also has great commercial value; it is no exaggeration to consider personal data to be the gold currency of the Information Age.

It is, therefore, fitting that the Senate Commerce Committee is examining Internet privacy. I am honored to be here today to share my views regarding privacy law in cyberspace.

There are three topics that I wish to address: (1) the European Data Protection Directive and the Safe Harbor Agreement; (2) the weaknesses in the current "market" for online privacy (the problem of "privacy market" failure); and, finally, (3) the nature of the privacy harms that individuals currently suffer in the online realm.

I. The European Data Protection Directive

The Member States of the European Union (E.U.) have enacted a Data Protection Directive that seeks both to harmonize their national data protection laws at a high level and to restrict transfers of personal data to third-party nations that lack "an adequate level of protection."[1] In cases where such adequate protection is not present, the Directive provides exceptions that permit transfers if, among other circumstances, the party receiving the data has agreed by contract to provide adequate protection.[2]

These national and European-wide measures for information privacy pose significant challenges to the free flow of personal data to the United States. Whether or not a U.S. company has "adequate" measures for information privacy requires examination of the protections available for specific data, including the safeguards offered by law and relevant business practices.[3] As a general matter, the European view regarding United States privacy law has been skeptical.[4]

In response to E.U. Data Protection Directive, the U.S. Commerce Department drafted and negotiated E.U. approval of "Safe Harbor" standards for privacy.[5] The Commerce Department sought to bridge differences in privacy approaches between the two countries and to "provide a streamlined means for U.S. organizations to comply with the Directive."[6] As the Commerce Department states, "The safe harbor — approved by the EU in July of 2000 — is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws."[7] Under Ambassador David Aaron's leadership, the Commerce Department also obtained E.U. agreement to waive sanctions against any American companies that follow these standards. American companies in the Safe Harbor are deemed to provide "adequate protection" for the personal data of Europeans.

What does the Safe Harbor provide? Americans companies that sign up for it promise to provide a range of Fair Information Practices for the personal information of Europeans. Fair Information Practices are the building blocks of modern information privacy law; they are centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent, that is open and understandable, processing systems; (3) limited procedural and substantive rights; and (4) external oversight.[8] These principles are not a European invention, but have been present in information privacy law and policy in the U.S. since the era of mainframe computers in the 1970's.

After a slow start for the Safe Harbor, more American companies are signing up for it. Perhaps the single most exciting development in the last year in U.S. privacy law has been this new willingness of corporate America to pledge allegiance to the most important Fair Information practices. Among the corporations now on the Safe Harbor list are Intel, Hewlett Packard, and Acxiom Data. Moreover, Microsoft has announced that it plans to sign on to the Safe Harbor agreement. These are, of course, all leading Information Technology corporations, and Acxiom is also a leading collector of personal data. Based in Little Rock, Arkansas, Acxiom Data supplies data infrastructure and technology services to help companies and organizations better understand customer behavior. It speaks well for the business compatibility of the Safe Harbor that these companies have agreed to it.

Under the terms of the Safe Harbor, however, American companies pledge to provide Fair Information Practices only for the personal data of European citizens. The question then becomes: why should American citizens be entitled under law only to a lesser level of privacy protection?

II. Weakness in the Current Privacy Market

In this part of my testimony, I wish to consider the foundation conditions for a functioning "privacy market" and to explore the weaknesses in the existing market for personal information.

A well-functioning privacy market requires sellers (i.e. consumers) to be able to bargain over the terms under which they will disclose their personal data, and buyers (i.e. data processors) to offer different packages and prices for this personal information. In such a market, "privacy price discrimination" will emerge. Privacy price discrimination involves a consumer seeking different packages of services, products, and money in exchange for her personal data, and a data processing company differentiating among consumers based both on their varying preferences about the use of their personal data and the underlying value of the information.

To illustrate this point, imagine two hypothetical consumers: Marc and Katie. Marc cares deeply about how his personal information is used; Katie does not. A surplus from cooperation under a property regime requires at a minimum, however, that Marc and others with similar preferences receive more than their "threat value" before disclosure. The term "threat value" refers to the "price" that Marc would place on *not* disclosing his personal information. Beyond receiving the threat value, privacy price discrimination also requires further elasticity in meeting more subtle privacy preferences of Marc. Under the current regime, however, companies generally have no need to offer Marc greater services or more money for his personal data than they offer Katie.

The failure in the privacy market can be attributed to at least four causes: (1) information asymmetries; (2) collective action problems; (3) bounded rationality; and (4) limits on "exit" from certain practices. We should briefly consider each of these four shortcomings in the privacy market.

A. Information Asymmetries

The first weakness in the privacy market is that most visitors to cyberspace lack essential knowledge of how their personal information will be processed or how technology will affect data collection. Due to this "knowledge gap," development through a privacy marketplace of rules for personal data use are likely to favor the entities with superior knowledge -- online industry rather than consumers. At present, even relatively basic Internet privacy issues, such as "cookies," are met with widespread consumer ignorance.

Cookies are alphanumerical files that Web sites place on the hard drives of their visitors' computers. Cookies are a ready source of detailed information about personal online habits, but consumers generally do not even know where cookie files are stored on their computer. Beyond

cookies, widespread information asymmetries involve other aspects of the Internet's technical infrastructure. As a result, "negotiations" about the use of personal information occur with one party, the consumer, generally unaware that bargaining is even taking place!

B. The Collective Action Problem

The second difficulty in the Internet privacy market is a collective action problem. The need is for individual privacy wishes to be felt collectively in the market. The good news first: a group of privacy-promoting organizations are emerging. Among these institutions are: (1) industry organizations that support self-regulation by drafting codes of conduct; (2) privacy seal organizations, such as TrustE and BBBOnline; (3) "infomediaries" that represent consumers by offering to exchange their data only with approved firms; (4) privacy watchdog organizations that bring developing issues to public attention; and (5) technical bodies, such as the World Wide Web Consortium (W3C), engaged in drafting Internet transmission standards, including the Platform for Privacy Preferences (P3P). P3P is a software transmission protocol that seeks to allow the individual to control her access to Web sites based on her privacy preferences and the practices at a given site.

Despite these promising developments, most of us are not yet able to free-ride successfully on the efforts of those who are more savvy about data privacy on the Internet. As many experts have pointed out, current collective solutions, such as industry self-regulation and privacy seals, are flawed. As an example, the FTC's 2000 Study, *Privacy Online*, points to the lack of effective enforcement in current models of industry self-regulation and the confusing implementation of privacy seal programs.[9] For that matter, the existence of competing privacy seal programs raises the risk of forum shopping by Web sites that are hoping for weaker enforcement from one seal service rather than the other.

C. Bounded Rationality

The third difficulty with the privacy market is "bounded rationality," a concept developed by behavior economists.[10] Scholarship in behavioral economics has demonstrated that consumers' general inertia towards default terms is a strong and pervasive limitation on free choice. This does not mean that consumers are all sheep, but it does mean that default rules and form terms can have great psychological force and are likely to reward those who otherwise have greater power.

As a result of this current power dynamic, individuals faced with standardized terms and expected to fend for themselves with available technology may simply accept whatever terms are offered by data processors. Indeed, the difficulties with bounded rationality extend not only to personal information as traditionally understood but a new and potentially risky set of personal information, namely "privacy meta-data." This point is worth elaborating.

Meta-data are information about information. For example, use of telecommunications now creates "communications attributes," which are valuable data about consumers' service and calling preferences (call waiting, caller ID, DSL lines, etc.). The use of privacy filtering technology, such as P3P, creates another kind of meta-data, namely information about one's privacy preferences.

Ironically, these meta-data will possibly contribute to additional privacy invasions. Already in the offline world, direct marketers generate and sell lists of people who have interest in protecting their privacy. *Filtering will therefore create the possibility of further privacy violations unless customers prove able not only to negotiate for their privacy but for the privacy of data about their privacy preferences.*

Bounded rationality points to the need to find ways to permit informed decision-making about use of one's personal information and personal meta-information at the least cost to a consumer. The risk is that the current privacy market will lead only to cyber-agreements that represent new kinds of contracts of adhesion. In other words, new technology may lead only to speedy ways to generate poor contracts.

D. Limits on Exit

Finally, cyberspace, in certain of its applications, turns out to be far from friction-free. In particular, when limits exist on "exit" from certain practices, the danger is that online industry will be able to "lock-in" a poor level of privacy on the Web. Again, cookies provide a good example — cookies demonstrate how privacy "lock-in" takes place. A ready source of detailed information about personal online habits and in widespread use, cookies are difficult to combat. Mastery of advanced settings on one's Web browser, the downloading of "cookie-cutting" software, and some public protests about more egregious practices have helped, but not solved this problem. As a joint paper of the Electronic Privacy and Information Center (EPIC) and Junkbusters has noted, "Those consumers, who have taken the time to configure their browsers to notify when receiving, or reject cookies, have found that web surfing becomes nearly impossible."[11]

Moreover, beyond cookies, the next privacy melt-down is never far away. A possible source for the next crisis are so-called "Web bugs," also known as "clear GIF," which permit Web sites to snoop on visitors by use of code that occupies only one pixel on the screen. To return to my earlier point about information asymmetries, an even lower level of consumer awareness exists about Web bugs than about cookies.

As a final example of the emerging "lock in" for informational privacy, many of us enter cyberspace anchored in real space settings that limit our ability to negotiate. The modern workplace demonstrates this phenomenon. As the NEW YORK TIMES concludes, "the debate over employee privacy is over."[12] It is over because "widespread, routine snooping on employees is no longer a threat but a fact."[13] Or, as BUSINESS WEEK states, "When it comes to privacy in the workplace, you don't have any."[14] The emerging Hobson's choice for Americans on the Internet is to sacrifice either privacy or access to the Internet.

*** ***

Let us conclude this section by returning to Marc and Katie, our two consumers with different privacy preferences. Due to the pervasive failure in the privacy market in the United States,

commercial entities generally obtain Marc's and Katie's personal data for the same low price. As a result, a subsidy is given to those data processing companies that exploit personal data. Put simply, the true "cost" of personal data is not charged these organizations. One likely result of subsidized personal information is that companies will over-invest in reaching consumers who do not wish to hear from them. Personal information at below-market costs will also lead companies to under-invest in technology that will enhance the expression of one's privacy preferences.

III. Economic and Non-Economic Harms Caused by Privacy Violations

It may be difficult at times to understand the nature of privacy harms that occur in cyberspace. And it is certainly true, as Professor Fred Cate and others have reminded us, that benefits are associated with the sharing of information.[15] Why should there be limits on the use of personal data? In my view, the nature of the harms to personal privacy on the Internet fall into two categories: (1) the economic, and (2) the non-economic.

A. Economic Harms

Privacy violations cause economic harms to consumers by: (1) causing an exchange of our personal information at lower rates than a fully functioning privacy market would permit; and (2) squelching democratic opportunity through emerging practices such as "Weblining." Finally, privacy violations also lead to: (3) a lack of consumer confidence that harms the development of e-commerce.

1. Personal Data at Below "Market" Rates

I have proposed that the true cost of personal data is not imposed on organizations — the personal data of consumers (the Marc's) who care about privacy and those that do not (the Katie's) can be obtained for the same price. This market failure leads to both deadweight losses and distributional consequences. The deadweight losses follow from the existence of consumers who would engage in more or different kinds of transactions on the Internet, but refuse to do so because of fears about how their personal data will be collected and used. Polls have consistently shown that many Americans decline to engage in cyberspace transactions because of such worries.[16] In this fashion, a deadweight loss reduces the economic surplus that would be created were privacy price discrimination in place. Such a loss, perhaps somewhat hidden during the Internet's early stages of rapid growth, will become more visible as e-commerce enters a slower stage. As a columnist in Silicon Valley's MERCURY CENTER warns, "almost all of the online retailers hurriedly launched in 1998 and 1999 now appear doomed to disappear — not because e-commerce isn't going to be important, but because consumers aren't moving fast enough toward online shopping to sustain today's Web retailers."[17]

The failure in the privacy market also involves a distribution away from Marc and even Katie and towards data processing companies. Companies have no need to offer Marc greater services or more money for his personal data. In fact, they may not even meet Katie's more modest privacy threat value.

2. Weblining and the Limiting of Opportunity

The benefits of access to information, including personal information, can certainly be positive. Yet, the processing of personal data can also create significant social risks. If used improperly, profiling will squelch opportunity rather than promote it. Consider the emerging practice of "Weblining," which is similar to "red-lining" in the real world. Weblining, as BUSINESS WEEK tells us, is the "Information Age version of that nasty old practice of redlining, where lenders and other businesses mark whole neighborhoods off-limits."[18] Weblining sews far-flung threads of personal data, including data about one's ethnic background or religion, into profiles that are used to sort people into categories and predict how they will behave. It creates segmenting in which it is our data profiles that decide the price that we pay, the services we obtain, and our access to new products and information. Weblining sometimes even relies on so-called "neural networks," which are digital systems that evolve over time in a fashion both independent of their developers and impossible to predict.

The danger is that Weblining will hinder or even reverse the kind of increased opportunity that access to information can stimulate. It can be used to limit economic and informational possibilities for individuals and different groups in a fashion that reflects and reinforces existing prejudices and mistaken beliefs. As BUSINESS WEEK warns, "Weblining may permanently close doors to you or your business."[19]

3. Consumer Uncertainty Harms the Development of E-Commerce

Americans may not fully understand the fashion in which Internet snooping occurs, but they do have a growing awareness that a privacy problem exists in cyberspace. As I have already noted above regarding the resulting deadweight losses, consumer worries about privacy are inhibiting electronic commerce. I wish to expand briefly on this point.

The Pew Research Center's "Internet and American Life" project furnishes insights into the dynamic of how the lack of Internet privacy harms e-commerce. The Pew Center's Internet Life Report, *Trust and privacy online* (August 20, 2000) found, first, that the leading fear of Internet users concerned their privacy. According to this survey, eighty-four percent of Internet users were worried about "[b]usinesses and people you don't know getting personal information about you and your family."[20] The Pew Research Center's report also noted that "[a] strong sense of distrust shades many Internet users view of the online world and the uneasiness has grown in the past two years."[21]

The Pew Research Center identified a relation between fears about privacy and "lower participation in some online activities, especially commercial and social activities."[22] In similar terms, a BUSINESS WEEK/Harris Poll from March 2000 found a high level of concern about privacy from people who have gone online but not yet shopped there.[23] Finally, the Forrester Research Group found in late 1999 that privacy concerns had led to $2.8 billion in lost sales that year alone.[24] Uncertainty about privacy is harming the development of e-commerce.

B. Non-Economic Harms

In addition to the economic harms that follow from the lack of strong privacy standards on the

Internet, non-economic harms also take place. Cyberspace is not only a place for shopping; it is our new arena for public and private activities. Cyberspace demonstrates information technology's great promise: to form new links between people and to marshall these connections to increase collaboration in political and other activities that promote democratic community. In particular, cyberspace has a tremendous potential to revitalize democratic self-governance at a time when a declining level of participation in communal life endangers civil society in the United States.

Consider the Supreme Court's decision in 1997 in *ACLU v. Reno*.[25] In striking down certain provisions of the Communication Decency Act, the Supreme Court declared its intention to protect the "vast democratic fora" of the Internet.[26] The Supreme Court considered the Internet to be a speaker's paradise; as the Court noted, "this dynamic, multifacted category of communication" permits "any person with a phone line" to "become a town crier with a voice that resonates farther than it could from any soapbox."[27] This language is similar to language used by the political scientist Benjamin Barber, who has defined civil society as the free space in which democratic attitudes are cultivated and conditioned.[28] In Professor Barber's words, "The public needs its town square."[29]

Without privacy, however, the implications of hanging out at the town square are dramatically changed. The Supreme Court's decision in *Reno v. ACLU* is also illustrative in this regard. The Supreme Court praised the Internet's potential for furthering free speech; for the Court, the Internet represented a "new marketplace of ideas."[30] We must note, however, a paradox in this regard: while listening to ideas offline, in Real Space, generally does not create a data trail, listening in cyberspace does. The Internet's interactive nature means that individuals on it simultaneously collect and transmit information; as a result, merely listening on the Internet becomes a speech-act. A visit to a Web site or a chat room generates a record of one's presence.

To extend the Supreme Court's metaphor, the role of town crier in cyberspace is often secretly assigned -- a person can take on this role, whether or not she seeks it or knows afterwards that she has been given it. Already a leading computer handbook, the *Internet Bible*, concludes its description of the low level of privacy in cyberspace with the warning, "Think about the newsgroups you review or join— they say a lot about you."[31] If cyberspace is to be a place where democratic discourse occurs, the right kinds of rules must shape the terms and conditions under which others have access to our personal data. The issue is of the highest importance; the Internet's potential to improve democracy will be squandered unless we safeguard the kinds of information use that democratic community requires.

A poor level of privacy in cyberspace threatens the promise of the Internet: it discourages political and social participation in this new realm. As Professor Jerry Kang has written of cyberspace, it is a place where "you are invisibly stamped with a bar code."[32] In the absence of strong privacy rules, Americans will hesitate to engage in cyberspace activities –- including those that are most likely to promote democratic self-rule.

Conclusion

The E.U. Data Protection Directive and the U.S. Commerce Department's Safe Harbor indicate a possibility of harmonizing global data flows at a high level of privacy protection. The question then becomes the kind of privacy protection that should be in place for personal data use within the U.S. In my testimony today, I have identified numerous grounds for concluding that the "privacy market," that is the market in which personal data are collected and exchanged in the U.S., will not alone produce the right level of information privacy. Finally, I have sought to identify a basic taxonomy of economic and non-economic harms occuring in the online realm. It is my hope that the Senate Commerce Committee will respond to this situation with introduction of strong consumer privacy legislation.

Thank you for the opportunity to testify today.

Biographical Information

PAUL M. SCHWARTZ is a Professor of Law at Brooklyn Law School (Brooklyn, New York). A leading international expert on informational privacy and information law, he has published and lectured in these areas in the United States and Europe.

In this country, his articles and essays have appeared in periodicals such as the STANFORD LAW REVIEW, COLUMBIA LAW REVIEW, TEXAS LAW REVIEW, and the AMERICAN JOURNAL OF COMPARATIVE LAW. His two-co-authored books are DATA PRIVACY LAW (1996, Supp. 1998), an in-depth study of the privacy protection provided for personal information in the United States, and DATA PROTECTION LAW AND ON-LINE SERVICES REGULATORY RESPONSES (1998), a study carried out for the Commission of the European Union that examines emerging issues in Internet privacy in four European countries.

Professor Schwartz has provided advice and testimony to numerous governmental bodies in the United States. He has also acted as an advisor to the Commission of the European Union on privacy issues. On behalf of the Practising Law Institute, he has served as co-chair for a series of Annual Institutes on Privacy Law in New York and San Francisco.

Before his appointment at Brooklyn Law School, Professor Schwartz taught at the University of Arkansas School of Law (Fayetteville) and visited at institutions including Boston College Law School and Case Western Reserve University Law School. Paul Schwartz is a graduate of Yale Law School, where he served as senior editor of the YALE LAW JOURNAL. He received his undergraduate education at Brown University.

Endnotes

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 25, O.J. of the European Communities, no.L281, 31 (Nov. 23, 1995) [hereinafter European Directive].

2. European Directive, at Art. 26.

3. European Directive, at Art. 25(2). *See* WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, FIRST ORIENTATIONS ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES - POSSIBLE WAYS FORWARD IN ASSESSING ADEQUACY, XV D/5020/97-EN final WP4 1-5 (June 26, 1997).

4. To make matters more complicated, the EU Directive's provisions on data transfers are enforced by the Member States, which makes their current views and future action critical.

5. INT'L TRADE ADMIN., ELECTRONIC COMMERCE TASK FORCE, SAFE HARBOR PRINCIPLES (Nov. 4, 1998) <http://www.ita.doc.gov/ecom/menu.htm>.

6. U.S. Commerce Dept, *Safe Harbor Overview*, (visited July 9, 2001) <http://www.export.gov.safehabor/SafeHarborInfo.html>.

7. *Id.*

8. For a description of early proposals regarding fair information practices, see THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 14-15, 500-502 (1977); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306-307 (1989).

For analysis of fair information practices as the building blocks of information privacy, see Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L.REV. 56-67 (1997); Paul M. Schwartz, *Privacy and Participation*, 80 IOWA L.REV. 563-564 (1995).

9. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (MAY 2000).

10. For citations to the relevant academic literature, see Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy*, 2000 WISC. L. REV. 744, 768-69.

11. Junkbusters & the Electronic Privacy Information Center, Pretty Poor Privacy: An Assessment of P3P and Internet Privacy 6 (June 2000) <http://www.junkbusters.com/ht/en/p3p.html>.

12. Jeffrey L. Seglin, *As Office Snooping Grows, Who Watches the Watchers?*, N.Y. TIMES, June 18, 2000, at Bus. Sec. 4.

13. *Id.*

14. Larry Armstrong, *Someone to Watch Over You*, BUSINESS WEEK, July 10, 2000, at 189.

15. See, e.g., Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000).

16. For a recent summary and discussion of the poll data, see FEDERAL TRADE COMMISSION, PRIVACY ONLINE 2 (May 2000). As the FTC states, "surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce, and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction." *Id.*

17. Mike Langberg, *Low cost net devices not about to push aside PC*, MERCURY CENTER, July 14, 2000.

18. Marcia Stepanek, *Weblining*, BUS. WK., Apr. 3, 2000, at 2. (http://www.businessweek.com/2000/00_14/b3675017.htm>.

19. *Id.*

20. Pew Internet & American Life Project, *Trust and privacy online* 4 (Aug. 20, 2000).

21. *Id.* at 12.

22. *Id.* at 16.

23. *BusinessWeek/Harris Poll: A Growing Threat*, BUS. WK., Mar. 20, 2000, at 1. <http://www.businessweek.com/2000/00_12/b3673010.htm>.

24. *Trails of Personal Info Compromise Net Shopper's Privacy*, USA TODAY, Dec. 20, 1999.

25. 117 S.Ct. 2329 (1997).

26. *Id.* at 2434.

27. Reno v. ACLU, 117 S.Ct. 2329, 2344 (1997).

28. BENJAMIN BARBER, A PLACE FOR US 76 (1998).

29. *Id.*

30. Reno, 117 S.Ct. at 2352.

31. BRIAN UNDERDAHL & EDWARD WILLETT, INTERNET BIBLE 247 (1998).

32. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998).